Game-Theoretic Strategies for Cyber-Physical Infrastructures Under Component Disruptions

Nageswara S. V. Rao, *Fellow, IEEE*, Chris Y. T. Ma, Fei He, *Member, INFORMS*

***Abstract*—Networked infrastructures of recursively defined systems composed of discrete cyber and physical components are considered. The components of basic systems at the finest levels can be disrupted by cyber or physical means, and can be reinforced to survive at certain costs. A problem of ensuring the infrastructure performance is formulated as a game between a provider and an attacker, who probabilistically choose components to reinforce and attack, respectively. The disruptions of this infrastructure are characterized using the aggregate failure correlation function that specifies the conditional failure probability of the infrastructure given the failure of an individual system at that level. The survival probabilities of basic systems satisfy simple product-form, first-order differential equations expressed in terms of the multiplier functions. The utility functions of the provider and attacker are composed of the reward and cost terms, both expressed in terms of the component reinforcement and attack probabilities. The Nash equilibrium of this game is characterized, along with the sensitivity functions of the survival probabilities of basic systems that highlight their dependence individually on the cost-benefit terms, the correlation functions, and the multiplier functions. These results are illustrated using simplified models of a distributed cloud servers infrastructure, a 5G data network infrastructure, a high performance computing federation, and a smart energy grid infrastructure.**

***Index Terms*—recursive system of systems, game theory, networked infrastructure, cloud servers infrastructure, 5G data network, high performance computing federation, energy grid**

I. Introduction

Infrastructures such as distributed cloud server farms, smart energy grids, and high performance computing (HPC) federations are complex networked systems. In addition, their individual systems by themselves are complex with several interdependent cyber and physical parts, and they consist of components at the finest levels. These infrastructures can be modeled as Recursive System of Systems (RSoS) that consist of multiple levels of systems as in [1]. In this paper, we consider their defense against the attacks on strategically chosen components; this formulation is at a finer scale compared to the bulk version in [1], where the attacker and provider choose an integer number of components to attack and reinforce, respectively. A RSoS can be expanded by recursively refining the systems into finer levels to end up at *basic* systems $S_b, b = 1, 2, \ldots, N_{\mathcal{S}}$, that consist entirely of discrete components. For example, in a distributed cloud servers infrastructure of 5 sites each with 10,000 servers, the sites and wide-area network can be modeled as top level systems, and they can be successively refined to reach basic systems with physical components such as computing servers, fiber lines, and network switches and routers, and also cyber components such as virtual machines, containers and operating systems [2].

The components of a basic system S_b must be *operational* by themselves and also be *available* such as being connected to the network to ensure the infrastructure performance. However, the individual components of S_b may be disabled and/or disconnected by cyber and physical disruptions, for example, in the cloud servers infrastructure, by cyber attacks on servers or unintended cuts to fiber lines. The effects of a disruption may propagate to other components within the basic system S_b; for example, cyber attacks may be launched on site servers from a compromised server. In addition, these effects may further propagate to components of other basic systems S_{b_1}, $b_1 \neq b$, due to various correlations. For instance, in the above infrastructure, a physical attack on a fiber line to a wide-area network router may result in all servers at multiple sites being unavailable. Thus, in addition to direct disruptions, the correlations within and between basic systems may render the components unavailable even if they are operational by themselves. In an extreme case, the effects of a component attack may propagate within its basic system and then to others, and eventually degrade the performance of the entire infrastructure.

In response to potential attacks, components may be reinforced to survive the disruptions and continue to provide services; for example, in the above infrastructure, replicated servers and redundant fiber lines ensure the continued service under single component disruptions. However, the component defences incur costs that must be balanced in view of the benefits; for example, in the case of cloud storage defense [3], more frequent checking by the provider reduces the impacts of

N. S. V. Rao is with the Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA. Email: raons@ornl.gov

C. Y. T. Ma is with the Department of Computing, The Hang Seng University of Hong Kong, Hong Kong. Email: chrisma@hsu.edu.hk

F. He is with the Department of Mechanical and Industrial Engineering, Texas A&M University-Kingsville, Kingsville, TX, USA. Email: fei.he@tamuk.edu

Manuscript received April 17, 2022; revised June 30, 2022; accepted August 7, 2022

This manuscript has been co-authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy (DOE). The US government retains and the publisher, by accepting the article for publication, acknowledges that the US government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for US government purposes. DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

0000–0000/00$00.00 © 2022 IEEE

persistent attacks but at an increased cost. These considerations naturally lead to game theoretic formulations [4], [5].

The infrastructure provider is tasked with strategically reinforcing the components against attacks by taking various correlations into account. We consider that components are reinforced and attacked by the provider and attacker of the infrastructure, respectively, using the probabilistic strategies. Let $\mathcal{S}_b = \{c_{b,1}, c_{b,2}, \ldots, c_{b,n_b}\}$ denote the set of n_b discrete components of a basic system S_b. Let $p_{c_{b,k}}$ and $q_{c_{b,k}}$ denote the probability of reinforcement and attack on the component $c_{b,k} \in \mathcal{S}_b$, $k = 1, 2, \ldots, n_b$, respectively. Then, let $P_{S_b} = (p_{c_{b,1}}, p_{c_{b,2}}, \ldots, p_{c_{b,n_b}})^T$ and $Q_{S_b} = (q_{c_{b,1}}, q_{c_{b,2}}, \ldots, q_{c_{b,n_b}})^T$ denote the corresponding reinforcement and attack probability vectors. Let $L_D(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}})$ and $L_A(Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}})$ denote the expected costs of reinforcements and attacks on the basic systems of the entire infrastructure, respectively. We then formulate a game between the provider and attacker wherein the provider minimizes the *utility function*, expressed as the sum of gain and cost product terms [4], given by

$$\begin{aligned} &U_D\left(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}, Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}\right) \\ &= F_{D,G}(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}, Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}) \\ &\quad \times G_D(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}, Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}) \\ &\quad + F_{D,L}(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}, Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}) \\ &\quad \times L_D(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}), \end{aligned} \tag{1}$$

where $F_{D,G}(\cdot)$ and $F_{D,L}(\cdot)$ are the *reward-multiplier* and *cost-multiplier* functions, respectively, of the provider, and $G_D(\cdot)$ represents the gain or reward of keeping the infrastructure operational. For example, under the advanced persistent threats formulation [6], $G_D(\cdot)$ may represent a quantity such as the data protection level. Similarly, the attacker's *utility function* is given by

$$\begin{aligned} &U_A\left(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}, Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}\right) \\ &= F_{A,G}(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}, Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}) \\ &\quad \times G_A(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}, Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}) \\ &\quad + F_{A,L}(P_{S_1}, \ldots, P_{S_{N_\mathcal{S}}}, Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}) \\ &\quad \times L_A(Q_{S_1}, \ldots, Q_{S_{N_\mathcal{S}}}), \end{aligned}$$

where $F_{A,G}(\cdot)$ and $F_{A,L}(\cdot)$ are the *reward-multiplier* and *cost-multiplier* functions, respectively, of the attacker, and $G_A(\cdot)$ represents the reward of disrupting the operation of the infrastructure.

To develop defense strategies for the provider, we characterize the disruptions at each level of recursion of this infrastructure between a system S_i^l at level l and the rest of the infrastructure that has the same parent system as S_i^l. A system survives when it is both *operational* and *available*. Let N_l be the number of level-l systems, $\mathcal{P}_I(S_i^l)$, or $\mathcal{P}_i^l$ in short, denote the survival probability of a basic or non-basic system S_i^l, $i \in \{1, 2, \ldots, N_l\}$, and $\mathcal{P}_I(\mathcal{S})$ denote the survival probability of the entire RSoS $\mathcal{S}$. For a system S_i^l with its parent system S_j^{l-1}, where $i \in \{1, 2, \ldots, N_l\}$ and $j \in \{1, 2, \ldots, N_{l-1}\}$, the *local aggregate failure correlation* C_i^l is the failure probability of the "rest" of the parent system (namely, S_j^{l-1} without S_i^l) given the failure of S_i^l. Intuitively, it indicates the relative importance of S_i^l by capturing the failure propagation from S_i^l to the other parts of the infrastructure under the same parent; in practice, such correlations are often estimated using the observations or measurements of the infrastructure without requiring a much deeper causal knowledge. For a basic system $S_b = S_i^l$, let $\mathcal{P}_I(S_b)$, or $\mathcal{P}_b$ in short, denote its survival probability, and C_b denote its local aggregate failure correlation. In addition to these system-level correlations, the interdependencies between the components are captured by a first-order differential condition using the *system multiplier function* of a basic system S_b [4]. This two-step characterization is natural in several energy and computing infrastructures [4], and it enables us to focus on critical parts of the infrastructure by "separating" the system- and component-level aspects. The RSoS hierarchy enables us to propagate the correlations across the levels, in particular, from components at different levels to the top infrastructure level. This combination of the *hierarchy and correlations* is a distinguished feature of our formulation, for example, compared to the single-level Stackelberg game of critical infrastructures in [7] and the aggregated cloud storage in [3].

In this paper, we derive the Nash Equilibrium (NE) conditions of this game by minimizing the utility functions with respect to the component attack and reinforcement probabilities [8], and present a succinct characterization of NE. These NE conditions show the dependence of $\mathcal{P}_I(\cdot)$ on cost and benefit terms of the provider, and also the infrastructure correlations and multiplier functions via a single succinct product term $\Delta_{\Pi_b}$for S_b (Lemma 5.1). We also derive a sensitivity function for the survival probability of the basic system $\mathcal{P}_b$ with respect to the component reinforcement probability $p_{c_b,k}$ that highlights the dependence on cost-benefit terms and their partial derivatives, and the correlation and multiplier functions (Theorem 5.1). Interestingly, it also indicates the sensitivity to the expected number of reinforced components of S_b denoted by $\bar{x}_b$, and the results in [1] form a special case.

The critical roles of individual components are better captured in the component-based game formulation of this paper compared to previous formulations based on the number of components [1], [4]; this is so despite the superficial similarities in the expressions for survival probability estimates (details in Section III). At a technical level, this probabilistic game formulation ensures the existence of NE and alleviates the large component size assumption needed for the existence of derivatives in other formulations. The resultant defense strategies are more focused on identifying and accounting for critical components located at possibly different RSoS levels, as illustrated in examples in Section VI.

The organization of this paper is as follows. We briefly describe the related work in Section II. In Section III, we describe a discrete component infrastructure model along with the correlation functions and differential conditions on the system survival probabilities; these definitions are generalizations of previous formulations [1], [4] which are based on the number of components. We present a component-based game formulation in Section IV, and derive NE conditions and sensitivity estimates in Section V. We also describe two special cases, OR systems in Section IV-A and statistically indepen-

dent sub-infrastructures in Section IV-B, wherein the analysis of correlation effects is somewhat simplified. We apply the analytical results to simple models of distributed cloud servers infrastructure, 5G data network infrastructure, HPC federation, and smart energy grid infrastructure in Section VI. We present conclusions in Section VII.

II. Related Work

Critical infrastructures that support energy, communication, computation, and transportation systems are vital to national security and economic well-being. These infrastructures are typically complex networked systems consisting of components that need to be protected against various intentional and incidental disruptions [9]–[12], and are often modeled as complex dynamic systems using partial differential equations to reflect the underlying physical properties [13]. The constituent components in critical infrastructures [11] can be typically categorized as cyber components, such as software for control and communication [2], [14], and physical components, such as hardware of sensors and actuators [15], [16]. Distributed cyber-physical systems (CPSs) typically entail recursive structures, for example, cloud computing infrastructures are composed of distributed servers, which are in turn composed of CPU and GPU nodes; traditional power grids are embedded with microgrids, which are composed of energy generation units, controllable device and energy storage units locally [17]; and autonomous vehicular clouds in which each vehicle is equipped with sensors, computing and data storage resources [18]. The recursive structures of CPSs have been explicitly incorporated into modeling and analyses of system functionality [1].

To counter the potential risks from external attacks and internal incidents in cyber-physical infrastructures [13], [19]–[21], it is critical to develop reinforcement strategies to maintain the functionality of CPS under these disruptions. Reliability and robustness analyses of CPS have been conducted using complex network theory [12], [22], [23], graph-theoretic network dynamics [24]–[26], game-theoretic and probabilistic modeling [6], [9], [27], with application to smart grids [28], computer network infrastructures [6], [29], [30], fuzzy dynamical systems [31], large scale industrial processes [32], cyber-physical control systems [33] and integrated multiple-infrastructure systems [34] (to name a few).

A main goal of an infrastructure provider is to ensure its continuous operation by countering attacks while balancing the defense costs, which naturally leads to game-theoretic utility formulations [35]–[38]. Game theory is typically applied to discover defense strategies by considering adaptive rationality of attackers [27], such as multiple-period games that address multiple time-scales of system dynamics [39]; defense against multiple attack technologies [40]; incomplete information games that account for partial knowledge about the system dynamics and attack [41]–[43]; game-theoretic strategies for resource allocation among multiple targets [44]–[49]; and cumulative prospect theory for subjective attackers and security agents of advanced persistent threats [6], [50]. A comprehensive review of the defense and attack strategies in various system structures using game-theoretic formulations has been presented in [51].

Game theory has also been widely used to improve performance of CPS recently, such as demand-side management [52] in smart grids with integration of electric vehicles and renewable energy [53], defense against cascading failures in power grids [54], intelligent transportation system considering human driving behavior [55], and smart medical services [56].

Although the works above address the functionality of specific infrastructures using game theory, they lack the generality to span multiple levels of complex networked infrastructures. This paper proposes a general framework for the game-theoretic protection of such infrastructures by exploiting the inherent recursive structure and correlations at various levels. Specifically, this paper addresses a class of networked infrastructures with discrete components using utility functions with cost and gain parts. It generalizes and unifies a series of previous works under this formulation in multiple directions: (i) the reinforcements and attacks on individual components generalize the formulations based on the number of components [1], [4], [5], (ii) RSoS characterization generalizes those based on fixed-level systems [57] and components [26], [58], (iii) the utility functions account for component reinforcement and attack probabilities, and encompass both sum and product forms [59], and (iv) the local aggregate correlations extend two-level system correlations to RSoS [4]. Also, this paper expands the illustrative examples of cloud servers infrastructure [60], HPC federation [61], and energy grid infrastructure [4] to encompass this component-based formulation.

From a broader perspective, our approach is related to a number of existing works but differs in certain details, specifically, in terms of objectives, formulation and solution methodology. Our overall performance objective based on incidental disruptions is similar to the reliability and availability characteristics of systems and infrastructures [62], and our analysis is similar to the risk analysis [63] of complex systems; our model, however, is a more generic cyber and physical system compared to the 2-level hierarchical model of multistage interconnect network in [64]. Our formulation of intentional disruptions can be viewed as a generalization of sorts of the byzantine generals problem [65] that considers the message compromises, and our analysis is similar to model-based analysis [66] of complex systems. Our RSoS tree is similar to attack trees [67] and is a specific version of the Markov models and fault trees [63], but is specifically designed to capture the correlations at different levels of the infrastructure. Our solution based on the game theory distinguishes it from these works, and the RSoS model distinguishes it from the single-level Markov models used in game theoretic analyses of electric and smart grids [68], [69].

III. Discrete Component Infrastructure Models

Several critical infrastructures can be modeled as RSoS consisting of multiple levels of systems with discrete components at the finest levels. Examples of distributed cloud servers infrastructure, 5G data network infrastructure, HPC

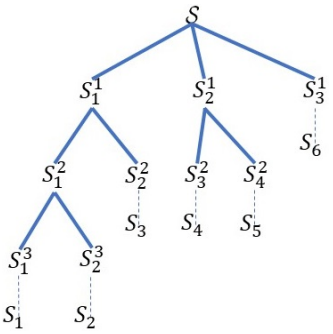


Fig. 1. RSoS tree representation of a simple infrastructure.

federation, and smart energy grid are described in Section VI. An abstract discrete component model has been developed for such infrastructures in terms of correlations and multiplier functions in [4], [5] and extended to RSoS based on the number of components in [1]. We describe extensions of these models in this section to account for the component-based game-theoretic formulation, which is at a finer level than the number of components[1].

A. RSoS Levels and Systems

A RSoS $\mathcal{S}$ [1] is either (i) a *basic* system composed of discrete cyber and physical components, or (ii) composed of N_1 level 1 systems $\mathcal{S}^1 = \{S_i^1 : i = 1, 2, \ldots, N_1\}$ listed from left to right, each of which is a recursively defined system of systems. Thus, $\mathcal{S}$ can be expanded as a *RSoS tree* by refining each non-basic system S_i^1 into next level systems S_j^2's, and so on. By recursively refining, we obtain the basic systems $\mathcal{S}^{\rm b} = \{S_b : b = 1, 2, \ldots, N_{\mathcal{S}}\}$, located at possibly different finest levels, which correspond to $N_{\mathcal{S}}$ leaves of the RSoS tree located at corresponding depths. We identify the set of systems $\mathcal{S}^l = \{S_i^l : i = 1, 2, \ldots, N_l\}$, listed from left to right at each level $l = 1, 2, \ldots, L$, which may consist of basic and non-basic systems (L is the deepest level of the tree). Thus, for each non-basic system S, we can identify its *descendant* basic systems $\mathcal{B}_S$ as the leaves of the RSoS subtree rooted at S.

A simple RSoS is depicted in Fig. 1 with six basic systems $S_1, S_2, \ldots, S_6$, which are also represented by leaf nodes $S_1^3, S_2^3, S_2^2, S_3^2, S_4^2, S_3^1$, respectively, in the other notation. Notice that RSoS tree structure captures the recursive decomposition of a complex infrastructure into subsystems, and it may not necessarily be a direct reflection of its network topology. In this simple RSoS, we have $\mathcal{S}^2 = \{S_1^2, S_3, S_4, S_5\}$. Here, $\mathcal{B}_{\mathcal{S}} = \mathcal{S}^{\rm b} = \{S_1, S_2, \cdots, S_6\}$ represents all basic systems of $\mathcal{S}$, and $\mathcal{B}_{S_1^2} = \{S_1, S_2\}$ represents the descendant basic systems of the non-basic system S_1^2.

Our current formulation and that using the number of components [1] are related as follows. For a basic system S_b, the expected number of components reinforced and attacked are denoted by $\bar{x}_b = \sum_{k=1}^{n_b} E\left[1_{D_{c_{b,k}}}\right]$ and $\bar{y}_b = \sum_{k=1}^{n_b} E\left[1_{A_{c_{b,k}}}\right]$, respectively, where $1_{D_{c_{b,k}}}$ and $1_{A_{c_{b,k}}}$ are indicator functions corresponding to the reinforcement and attack of the component $c_{b,k}$, respectively, of the basic system S_b.

[1]For completeness, some of the definitions are presented as in their original form with references, while others are adapted to the current component-based game formulation.

B. Aggregate Correlation Function

At each level l of the infrastructure, we capture the interactions between the systems in terms of survival probabilities using the local aggregate failure correlation function [4]. Let $\mathcal{S}^l_{-S_i^l}$ denote the part of infrastructure at level l without S_i^l that has the same parent system as S_i^l in the RSoS tree, where $i \in \{1, 2, \ldots, N_l\}$, and $\mathcal{P}_I\left(\mathcal{S}^l_{-S_i^l}\right)$ be its survival probability.

Condition 3.1: **Local Aggregate Failure Correlation Function** [4]: The probability that sub-RSoS $\mathcal{S}_j^l$, $j \in \{1, 2, \ldots, N_{l-1}\}$, representing a parent system at level $l-1$ that has level-l system S_i^l, $i \in \{1, 2, \ldots, N_l\}$, as its child system, is operational and available is given by

$$\mathcal{P}_I(\mathcal{S}_j^l) = \mathcal{P}_I(S_i^l) + \mathcal{P}_I\left(\mathcal{S}^l_{-S_i^l}\right) - 1 + C_i^l \left(1 - \mathcal{P}_I(S_i^l)\right), \quad (2)$$

where

$$C_i^l = C_{-i}^l \left(\frac{1 - \mathcal{P}_I\left(\mathcal{S}^l_{-S_i^l}\right)}{1 - \mathcal{P}_I(S_i^l)} \right)$$

is the *local aggregate failure correlation* of system S_i^l. □

Here, $\mathcal{P}_I(\mathcal{S}) = \mathcal{P}_I(\mathcal{S}^1)$ is the survival probability of the infrastructure. This definition can be recursively applied to express $\mathcal{P}_I(S_i^l)$ in terms of $\mathcal{P}_I(\cdot)$'s of descendants of S_i^l and the local aggregate correlations corresponding to level l and below. The local aggregate failure correlation function captures the interdependence of rest of the system $\mathcal{S}^l_{-S_i^l}$ on the failure of S_i^l. In a special case, the failure of S_i^l leads to a definite failure of the rest of the infrastructure; for example, the failure of the communications network renders all supercomputers of a HPC federation unavailable to remote users. Here, we have $C_i^l = 1$ such that $\mathcal{P}_I(\mathcal{S}) = \mathcal{P}_I\left(\mathcal{S}^l_{-S_i^l}\right)$, that is, the survival probability solely depends on $\mathcal{S}^l_{-S_i^l}$.

The effects of component reinforcements on the survival probabilities of systems at various levels are reflected in the partial derivatives with respect to reinforcement probabilities. At each level l, we consider the condition $\frac{\partial \mathcal{P}_I\left(\mathcal{S}^l_{-S_i^l}\right)}{\partial p_{c_{b,k}}} = 0$, where S_b is a descendant basic system of S_i^l with component $c_{b,k}$ (i.e., $S_b \in \mathcal{B}_{S_i^l}$ and $c_{b,k} \in \mathcal{S}_b$). This condition indicates that reinforcement of a component of S_b does not directly impact the survival probability of the rest of RSoS $\mathcal{S}^l_{-S_i^l}$, since S_b is not reachable through the recursive expansion of other systems S_j^l, for $j \neq i$. We capture such system-level considerations at each level for the provider using the following generalization of the condition in [1] to system components.

Condition 3.2: **De-Coupled Reinforcement Aggregate Effects:** For $\mathcal{P}_I(\mathcal{S}_j^l)$, $j = 1, 2, \ldots, N_{l-1}$, in Condition 3.1, we have for systems S_i^l, $i = 1, 2, \ldots, N_l$, of level l

$$\frac{\partial \mathcal{P}_I(\mathcal{S}_j^l)}{\partial p_{c_{b,k}}} = \left(1 - C_i^l\right) \frac{\partial \mathcal{P}_I(S_i^l)}{\partial p_{c_{b,k}}} + \left(1 - \mathcal{P}_I(S_i^l)\right) \frac{\partial C_i^l}{\partial p_{c_{b,k}}}, \quad (3)$$

where S_b is a basic system of S_i^l with component $c_{b,k}$. □

This condition can be recursively applied to express $\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}}$ for the entire infrastructure in terms of $\frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}}$ and $\mathcal{P}_I(S_b)$ of basic systems, and the aggregate failure correlation functions at levels l through L as will be shown in Lemma 5.1.

C. Basic Systems and Components

A basic system S_b solely consists of components and cannot be further recursively refined. Thus, $\mathcal{P}_I(S_b)$ depends on the correlations between the components within each S_b in addition to its aggregate correlation. These component correlations are characterized by the multiplier function of survival probabilities of basic systems that satisfy the following differential condition.

Condition 3.3: **System Multiplier Functions for Basic Systems:** The survival probability $\mathcal{P}_I(S_b)$ of a basic system S_b, $b = 1, 2, \ldots, N_{\mathcal{S}}$, satisfies the following condition: there exists a *basic system multiplier function* $\Lambda_b(\cdot)$ such that

$$\frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} = \Lambda_b \left(P_{X_1}, \ldots, P_{X_{N_{\mathcal{S}}}}, Q_{Y_1}, \ldots, Q_{Y_{N_{\mathcal{S}}}} \right) \mathcal{P}_I(S_b), \tag{4}$$

where $c_{b,k}$ is a component of S_b. □

This condition generalizes an earlier version defined using the number of components [5]. The basic system multiplier functions are defined for basic systems which can be at different levels, whereas Condition 3.2 is defined for systems at the same level l. As an example, consider the contest success functions [70], [71] that model the survival probability of a basic system S_b as $\mathcal{P}_I(S_b) = \frac{\xi + \bar{x}_b}{\xi + \bar{x}_b + \bar{y}_b}$, in terms of the inherent defense level ξ and the expected number of components reinforced and attacked. The basic system multiplier function can then be obtained from the following equation

$$\begin{aligned} \frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} &= \frac{\partial \mathcal{P}_I(S_b)}{\partial \bar{x}_b} \frac{\partial \bar{x}_b}{\partial p_{c_{b,k}}} \\ &= \left[\frac{\bar{y}_b}{(\xi + \bar{x}_b + \bar{y}_b)(\xi + \bar{x}_b)} \right] \mathcal{P}_I(S_b), \end{aligned}$$

since $\frac{\partial \bar{x}_b}{\partial p_{c_{b,k}}} = 1$.

We express the survival probability of the infrastructure in term of the correlations and multiplier conditions for all basic systems in the following condition.

Condition 3.4: **Correlations and De-Coupled Reinforcement Conditions for Basic Systems:** For a basic system S_b of $\mathcal{S}$ at level $m_b + 1$ with its parent system $S^{m_b}_{b_{m_b}}$, $b_{m_b} \in \{1, 2, \ldots, N_{m_b}\}$, in the RSoS tree, the conditions corresponding to Conditions 3.1 and 3.2 are given by:

$$\mathcal{P}_I \left(S^{m_b}_{b_{m_b}} \right) = \mathcal{P}_I(S_b) + \mathcal{P}_I \left(\mathcal{S}^{m_b+1}_{-S_b} \right) - 1 + C_b \left[1 - \mathcal{P}_I \left(S_b \right) \right],$$

where C_b is the local aggregate failure correlation function of system S_b, and

$$\frac{\partial \mathcal{P}_I \left(S^{m_b}_{b_{m_b}} \right)}{\partial \bar{x}_b} = (1 - C_b) \frac{\partial \mathcal{P}_I(S_b)}{\partial \bar{x}_b} + (1 - \mathcal{P}_I(S_b)) \frac{\partial C_b}{\partial \bar{x}_b},$$

respectively, for $b = 1, 2, \ldots, N_{\mathcal{S}}$. For the entire infrastructure $\mathcal{S}$, we consider

$$\mathcal{P}_I \left(\mathcal{S} \right) = \mathcal{P}_I(S_b) + \mathcal{P}_I \left(\mathcal{S}_{-S_b} \right) - 1 + \bar{C}_b \left[1 - \mathcal{P}_I \left(S_b \right) \right], \tag{5}$$

where $\bar{C}_b$ is the *global aggregate failure correlation* of S_b and $\mathcal{S}_{-S_b}$ is the rest of the infrastructure without S_b.□

A more general version of this condition can be derived for any part of the infrastructure represented by system S^l_i at level l by expressing $\mathcal{P}_I(S^l_i)$ in terms of the corresponding basic systems $S_b \in \mathcal{B}_{S^l_i}$.

IV. Game Theoretic Formulation

The provider's objective is to sustain infrastructure performance by probabilistically reinforcing the components of basic systems S_b, $b = 1, 2, \ldots, N_{\mathcal{S}}$, as determined by the minimization of the utility function $U_D(\cdot)$. Similarly, the attacker's objective is to disrupt the infrastructure by probabilistically attacking the components of S_b as determined by the minimization of the corresponding utility function $U_A(\cdot)$. For brevity, we only show the derivation of the NE conditions for the provider. However, those for the attacker can be similarly determined.

NE conditions are derived by equating the derivatives of the utility function (Eq. 1) with respect to the component reinforcement probability to zero, which yields [72]

$$\begin{aligned} \frac{\partial U_D}{\partial p_{c_{b,k}}} = \left(G_D \frac{\partial F_{D,G}}{\partial \mathcal{P}_I(\mathcal{S})} + L_D \frac{\partial F_{D,L}}{\partial \mathcal{P}_I(\mathcal{S})} \right) \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} \\ + F_{D,G} \frac{\partial G_D}{\partial p_{c_{b,k}}} + F_{D,L} \frac{\partial L_D}{\partial p_{c_{b,k}}} = 0 \end{aligned}$$

for $b = 1, 2, \ldots, N_{\mathcal{S}}$, $k = 1, 2, \ldots, n_b$, for the provider. We define the *composite gain-cost* given by

$$L^D_{G,L} \triangleq G_D \frac{\partial F_{D,G}}{\partial \mathcal{P}_I(\mathcal{S})} + L_D \frac{\partial F_{D,L}}{\partial \mathcal{P}_I(\mathcal{S})},$$

which consists of the gain and cost terms scaled with the derivatives of their corresponding multiplier functions with respect to $\mathcal{P}_I(\mathcal{S})$. We also define the *gain-cost gradient* given by

$$\begin{aligned} F^{D,b}_{G,L} &\triangleq F_{D,G} \frac{\partial G_D}{\partial p_{c_{b,k}}} + F_{D,L} \frac{\partial L_D}{\partial p_{c_{b,k}}} \\ &= F_{D,G} \frac{\partial G_D}{\partial \bar{x}_b} + F_{D,L} \frac{\partial L_D}{\partial \bar{x}_b} \end{aligned}$$

which consists of the multiplier functions scaled with the derivatives of their corresponding gain and cost terms with respect to $p_{c_{b,k}}$, $b = 1, 2, \ldots, N_{\mathcal{S}}$, $k = 1, 2, \ldots, n_b$, and to $\bar{x}_b$, as $\frac{\partial \bar{x}_b}{\partial p_{c_{b,k}}} = 1$. Hence, at NE we have the following simplified condition on the partial derivative

$$\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} = -\frac{F^{D,b}_{G,L}}{L^D_{G,L}} \triangleq -\Theta_b \left(P_{X_1}, \ldots, P_{X_{N_{\mathcal{S}}}}, Q_{Y_1}, \ldots, Q_{Y_{N_{\mathcal{S}}}} \right), \tag{6}$$

where $\Theta_b(\cdot)$ denotes the *scaled gain-cost gradient* of basic system S_b. For brevity, we denote $\Lambda_b \left(P_{X_1}, \ldots, P_{X_{N_{\mathcal{S}}}}, Q_{Y_1}, \ldots, Q_{Y_{N_{\mathcal{S}}}} \right)$ by Λ_b, and $\Theta_b \left(P_{X_1}, \ldots, P_{X_{N_{\mathcal{S}}}}, Q_{Y_1}, \ldots, Q_{Y_{N_{\mathcal{S}}}} \right)$ by Θ_b, for $b = 1, 2, \ldots, N_{\mathcal{S}}$.

We next consider two cases wherein specific forms of correlations lead to simplified NE conditions.

A. Local and Global OR Infrastructures

The OR systems [4] represent infrastructures where simultaneous failures of two or more systems are extremely unlikely at each level. These systems are simpler to analyse due to the absence of system-level correlation terms.

For a *global OR infrastructure*, the failure of a basic system does not impact the rest of the infrastructure $\mathcal{S}$ such that $\bar{C}_b = 0$, for $b = 1, 2, \ldots, N_{\mathcal{S}}$, and hence $\mathcal{P}_I(\mathcal{S}) = \mathcal{P}_I(S_b) + \mathcal{P}_I(\mathcal{S}_{-S_b}) - 1$. In these (theoretical) systems, for $k = 1, 2, \ldots, n_b$, we have

$$\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} = \frac{\partial \mathcal{P}_b}{\partial p_{c_{b,k}}} = -\frac{F^{D,b}_{G,L}}{L^{D}_{G,L}} = -\Theta_b.$$

Then, Condition 3.3 (Eq. 4) provides an estimate $\check{\mathcal{P}}_{b;D}$ of the survival probability $\mathcal{P}_I(S_b) = \mathcal{P}_b$ of S_b for the provider, given by

$$\check{\mathcal{P}}_{b;D} = -\frac{\Theta_b}{\Lambda_b},$$

for $b = 1, 2, \ldots, N_{\mathcal{S}}$. This estimate depends mainly on the scaled gain-cost gradient of S_b, and thus represents its "separation" from other basic systems. In this sense, OR systems constitute an important analytical case wherein correlations between the individual systems may be ignored. Although the estimates do not directly involve $\bar{C}_b$, the interactions between basic systems can still be captured by $\Lambda_b(\cdot)$ and $\Theta_b(\cdot)$ which in general depend on other basic systems.

A *local OR infrastructure* is defined by a weaker condition that $C_b = 0$, which implies $\mathcal{P}_I\left(S^{m_b}_{b_{m_b}}\right) = \mathcal{P}_I(S_b) + \mathcal{P}_I\left(\mathcal{S}^{m_b+1}_{-S_b}\right) - 1$.

The cloud memory defense formulation in [3] can be modeled as a single-level OR infrastructure; under the assumption of a single site attack or incidental disruption, the failure of storage at one site does not affect the other ($C_b = 0$), and the sum of the surviving storage can be incorporated into the provider's utility function. We can observe that the survival probability $\check{\mathcal{P}}_{b;D}$ is inversely proportional to the weighted gain term and proportional to its derivative; this seemingly counterintuitive trend is applicable to solutions constrained by Nash equilibria conditions, and not to the unconstrained infrastructure.

B. Statistical Independence of Systems

We consider that the failures of basic system S_b and the rest of the infrastructure $\mathcal{S}_{-S_b}$ are statistically independent such that $\mathcal{P}_I(\mathcal{S}) = \mathcal{P}_I(\mathcal{S}_{-S_b})\mathcal{P}_I(S_b)$. Based on Condition 3.4 (Eq. 5) for $\mathcal{S}$, we have $\bar{C}_b = 1 - \mathcal{P}_I(\mathcal{S}_{-S_b})$. Using $\frac{\partial \mathcal{P}_I\left(\mathcal{S}_{-S_b}\right)}{\partial p_{c_{b,k}}} = 0$, at NE we have

$$\mathcal{P}_I(\mathcal{S}_{-S_b})\frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} = -\Theta_b.$$

Applying Condition 3.3 (Eq. 4), at NE we have an estimate for the survival probability of S_b given by

$$\bar{\mathcal{P}}_{b;D} = -\frac{\Theta_b}{\Lambda_b}\frac{1}{\mathcal{P}_I(\mathcal{S}_{-S_b})}.$$

Similar to OR systems, the estimate $\bar{\mathcal{P}}_{b;D}$ for statistically independent systems is inversely proportional to the corresponding weighted cost and reward functions, and proportional to their weighted derivatives. However, unlike OR systems, statistical independence is not sufficient to decouple the estimate $\bar{\mathcal{P}}_{b;D}$ from $\mathcal{P}_I(\mathcal{S}_{-S_b})$, i.e., to depend solely on $\Lambda_b(\cdot)$ and $\Theta_b(\cdot)$. In particular, the estimate $\bar{\mathcal{P}}_{b;D}$ is inversely proportional to the survival probability of the rest of the infrastructure at NE.

V. NE Sensitivity Functions: Aggregate Correlations

We now derive estimates for the survival probability $\mathcal{P}_I(S_b)$ of basic system S_b at NE using partial derivatives of the cost and failure correlation functions with respect to $p_{c_{b,k}}$, the reinforcement probability of the component $c_{b,k}$ of S_b. For that purpose, we express the term $\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}}$ by recursively applying Condition 3.2 (Eq. 3), followed by Condition 3.3 (Eq. 4), for the corresponding S_b's, for $b = 1, 2, \ldots, N_{\mathcal{S}}$, $k = 1, 2, \ldots, n_b$.

Lemma 5.1: **Propagation of Correlations and Multiplier Functions:** Consider a component $c_{b,k}$ of the basic system S_b obtained by recursively expanding the RSoS $\mathcal{S}$. Let the path from $\mathcal{S}$ to the leaf S_b at level m_b+1 consists of the sequence of recursively expanding systems $\mathcal{S}, S^1_{b_1}, S^2_{b_2}, ..., S^{m_b}_{b_{m_b}}, S_b$.

(i) By extending the correlation functions and survival probability functions, with Condition 3.2 (Eq. 3) recursively applied until S_b, we have

$$\begin{aligned}\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} = &\left(1 - C_{\prod_b}\right)\frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} \\ &+ \Delta_{\prod_b}\left(\left(1 - \mathcal{P}_I(S_b)\right)\frac{\partial C_b}{\partial p_{c_{b,k}}}\right) + \frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}},\end{aligned} \tag{7}$$

where

$$\Delta_{\prod_b} = \prod_{l=1}^{m_b}\left(1 - C^l_{b_l}\right),$$

$$\begin{aligned}\frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}} = &\sum_{l=2}^{m_b}\left(\frac{\partial C^l_{b_l}}{\partial p_{c_{b,k}}}\left(1 - \mathcal{P}_I(S^l_{b_l})\right)\prod_{j=1}^{l-1}\left(1 - C^j_{b_j}\right)\right) \\ &+ \left(1 - \mathcal{P}_I(S^1_{b_1})\right)\frac{\partial C^1_{b_1}}{\partial p_{c_{b,k}}},\end{aligned}$$

and $C_{\prod_b}$ is the *product aggregate correlation function* given by

$$C_{\prod_b} = 1 - (1 - C_b)\prod_{l=1}^{m_b}\left(1 - C^l_{b_l}\right). \tag{8}$$

(ii) In terms of the *product multiplier function* $\Lambda_{\prod_b}$ of S_b given by

$$\Lambda_{\prod_b} = \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial \mathcal{P}_I(S^1_{b_1})}\frac{\partial \mathcal{P}_I(S^1_{b_1})}{\partial \mathcal{P}_I(S^2_{b_2})}\cdots\frac{\partial \mathcal{P}_I\left(S^{m_b}_{b_{m_b}}\right)}{\partial \mathcal{P}_I(S_b)}\Lambda_b, \tag{9}$$

we have

$$\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} = \Lambda_{\prod_b}\mathcal{P}_I(S_b). \tag{10}$$

Proof: To show Part (i), we apply Condition 3.2 (Eq. 3) to $S^1_{b_1}, S^2_{b_2}, ..., S^{m_b}_{b_{m_b}}, S_b$ such that

$$\begin{aligned}
\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} &= \left(1 - C^1_{b_1}\right) \frac{\partial \mathcal{P}_I(S^1_{b_1})}{\partial p_{c_{b,k}}} + \left(1 - \mathcal{P}_I(S^1_{b_1})\right) \frac{\partial C^1_{b_1}}{\partial p_{c_{b,k}}} \\
\frac{\partial \mathcal{P}_I(S^1_{b_1})}{\partial p_{c_{b,k}}} &= \left(1 - C^2_{b_2}\right) \frac{\partial \mathcal{P}_I(S^2_{b_2})}{\partial p_{c_{b,k}}} + \left(1 - \mathcal{P}_I(S^2_{b_2})\right) \frac{\partial C^2_{b_2}}{\partial p_{c_{b,k}}} \\
\frac{\partial \mathcal{P}_I(S^2_{b_2})}{\partial p_{c_{b,k}}} &= \left(1 - C^3_{b_3}\right) \frac{\partial \mathcal{P}_I(S^3_{b_3})}{\partial p_{c_{b,k}}} + \left(1 - \mathcal{P}_I(S^3_{b_3})\right) \frac{\partial C^3_{b_3}}{\partial p_{c_{b,k}}} \\
\cdots &= \cdots \\
\frac{\partial \mathcal{P}_I\left(S^{m_b}_{b_{m_b}}\right)}{\partial p_{c_{b,k}}} &= (1 - C_b) \frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} + (1 - \mathcal{P}_I(S_b)) \frac{\partial C_b}{\partial p_{c_{b,k}}}.
\end{aligned}$$

Then by repeatedly substituting the above equations, we obtain

$$\begin{aligned}
\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} = &\left(1 - C_{\prod_b}\right) \frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} \\
&+ \left(1 - \mathcal{P}_{\prod_b}(S_b)\right) \frac{\partial C_b}{\partial p_{c_{b,k}}} \\
&+ \sum_{l=2}^{m_b} \left(\frac{\partial C^l_{b_l}}{\partial p_{c_{b,k}}} \left(1 - \mathcal{P}_I(S^l_{b_l})\right) \prod_{j=1}^{l-1} \left(1 - C^j_{b_j}\right) \right) \\
&+ \left(1 - \mathcal{P}_I(S^1_{b_1})\right) \frac{\partial C^1_{b_1}}{\partial p_{c_{b,k}}},
\end{aligned}$$

where

$$1 - \mathcal{P}_{\prod_b}(S_b) = (1 - \mathcal{P}_I(S_b)) \prod_{l=1}^{m_b} \left(1 - C^l_{b_l}\right) = \Delta_{\prod_b}(1 - \mathcal{P}_I(S_b)).$$

Part (ii) follows by applying the chain rule to $\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}}$ in terms of $\mathcal{P}_I(\cdot)$'s of $\mathcal{S}, S^1_{b_1}, S^2_{b_2}, ..., S^{m_b}_{b_{m_b}}, S_b$ and then applying Condition 3.3 (Eq. 4). □

Qualitative information about the sensitivities of $\mathcal{P}_I(S_b)$ to different parameters can be inferred using estimates derived in the following result.

Theorem 5.1: **Basic System Survival Probability Estimates:** Under Conditions 3.1, 3.2 and 3.3, the estimates $\hat{\mathcal{P}}_{b;D}$ and $\tilde{\mathcal{P}}_{b;D}$ of the survival probability $\mathcal{P}_I(S_b)$ of basic system S_b expressed in terms of $C_{\prod_b}$ and $\Lambda_{\prod_b}$, respectively, for $b = 1, 2, \ldots, N_{\mathcal{S}}$, are given by

$$\hat{\mathcal{P}}_{b;D} = \frac{\Delta_{\prod_b} \frac{\partial C_b}{\partial p_{c_{b,k}}} + \frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}} + \frac{F^{D,b}_{G,L}}{L^D_{G,L}}}{\Delta_{\prod_b} \frac{\partial C_b}{\partial p_{c_{b,k}}} - \left(1 - C_{\prod_b}\right) \Lambda_b} \tag{11}$$

where S_b is a basic system under the condition: $\Delta_{\prod_b} \neq 0$ and $\frac{\partial C_b}{\partial p_{c_{b,k}}} - (1 - C_b)\Lambda_b \neq 0$, and

$$\tilde{\mathcal{P}}_{b;D} = -\frac{1}{\Lambda_{\prod_b}} \frac{F^{D,b}_{G,L}}{L^D_{G,L}}.$$

Proof: Our proof is based on deriving NE conditions for the utility function. At NE (Eq. 6), we have

$$\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} = -\frac{F^{D,b}_{G,L}}{L^D_{G,L}}.$$

The proof follows along the lines of [1], and we provide the details here for completeness. Using Part (i) of Lemma 5.1 (Eq. 7), we have

$$\begin{aligned}
\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} &= (1 - C_{\prod_b}) \frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} \\
&\quad + \Delta_{\prod_b} \left((1 - \mathcal{P}_I(S_b)) \frac{\partial C_b}{\partial p_{c_{b,k}}} \right) + \frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}}, \\
&= -\frac{F^{D,b}_{G,L}}{L^D_{G,L}}.
\end{aligned}$$

Then, by Condition 3.3 (Eq. 4), we have $\frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} = \Lambda_b \mathcal{P}_I(S_b)$. Denoting estimate of $\mathcal{P}_I(S_b)$ by $\hat{\mathcal{P}}_{b;D}$, we have

$$\begin{aligned}
&(1 - C_{\prod_b})\Lambda_b \hat{\mathcal{P}}_{b;D} + \Delta_{\prod_b} \left(1 - \hat{\mathcal{P}}_{b;D}\right) \frac{\partial C_b}{\partial p_{c_{b,k}}} \\
&\qquad = -\left(\frac{F^{D,b}_{G,L}}{L^D_{G,L}} + \frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}} \right).
\end{aligned}$$

Under the condition $\Delta_{\prod_b} \neq 0$ and $\frac{\partial C_b}{\partial p_{c_{b,k}}} - (1 - C_b)\Lambda_b \neq 0$, we have

$$\Delta_{\prod_b} \frac{\partial C_b}{\partial p_{c_{b,k}}} - \left(1 - C_{\prod_b}\right) \Lambda_b \neq 0,$$

which provides the above expression for $\hat{\mathcal{P}}_{b;D}$. The second estimate $\tilde{\mathcal{P}}_{b;D}$ follows from Part (ii) of Lemma 5.1 (Eq. 10). □

The system survival probability estimate $\hat{\mathcal{P}}_{b;D}$ of basic system S_b provides qualitative information about the effects of various parameters including the product aggregate correlation coefficient $C_{\prod_b}$, basic system multiplier function $\Lambda_b(\cdot)$, composite gain-cost $L^D_{G,L}$ and gain-cost gradient $F^{D,b}_{G,L}$. We note that these estimates may not necessarily lie within range [0,1], and their main purpose here is to illustrate the dependencies of various terms while others are fixed. In particular, $\hat{\mathcal{P}}_{b;D}$ (i) increases and decreases with $F^{D,b}_{G,L}$ and $L^D_{G,L}$, respectively, (ii) increases with $\Lambda_b(\cdot)$, and (iii) depends directly on both C_b and its derivative for $b = 1, 2, \ldots, N_{\mathcal{S}}$, and indirectly on the corresponding correlations and derivatives at different levels of recursion. The effects of $p_{c_{b,k}}$ on the survival probability are captured succinctly by $\Lambda_b(\cdot)$, the failure correlation functions and their derivatives. The component-level correlations of S_b are captured succinctly by the product $\left(1 - C_{\prod_b}\right) \Lambda_b$, with no effect of Λ_b when S_b affects the rest of infrastructure ($C_b = 1$) and full effect for OR systems ($C_b = 0$).

The second estimate $\tilde{\mathcal{P}}_{b;D}$ has a much simpler form but it subsumes correlations at all levels of recursion that correspond to S_b via its product multiplier function $\Lambda_{\prod_b}$, which depends on the partial derivatives of $\mathcal{P}_I(\cdot)$'s at successive levels as indicated in Part (ii) of Lemma 5.1.

By using $\frac{\partial C_b}{\partial p_{c_{b,k}}} = \frac{\partial C_b}{\partial \bar{x}_b}$ and $\frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}} = \frac{\partial C_{\Delta_b}}{\partial \bar{x}_b}$ in the expression for $\hat{\mathcal{P}}_{b;D}$, qualitative inferences can be made in terms of $\bar{x}_b$, the expected number of components reinforced. Thus, these survival probability estimates also indicate sensitivity to the expected number of components reinforced.

When applied directly to a RSoS $\mathcal{S}$ that consists of only basic systems S_b (namely, with 0 level of recursion, or $m_b =$

0), this theorem provides a simpler expression derived for SoS than in [72]

$$\hat{\mathcal{P}}_{b;D} = \frac{\frac{\partial C_b}{\partial p_{c_{b,k}}} + \frac{F^{D,b}_{G,L}}{L^D_{G,L}}}{\frac{\partial C_b}{\partial p_{c_{b,k}}} - (1 - C_b)\Lambda_b},$$

wherein we have $\Delta_{\prod_b} = 1$, $\Lambda_{\prod_b} = \Lambda_b$, $C_{\prod_b} = C_b = \bar{C}_b$ and $\frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}} = 0$. The added generality of the recursive formulation of RSoS still preserves the basic form of the estimate $\hat{\mathcal{P}}_{b;D}$ valid for the simpler SoS formulation, albeit under the expanded definitions of the product aggregate correlation function and the product multiplier function.

A. Expected Capacity

Let $\mathcal{C}_b \subseteq \mathcal{S}_b$ be a subset of *core* components of the basic system S_b that represent *core* resources of the infrastructure. For example, the *core* resources of distributed cloud servers infrastructure and HPC may represent the capacity of the server computers and computing nodes, respectively, and those of 5G network may represent the number of mobile users or the aggregate data rate. The core resource of the transmission system of a smart energy grid is the capacity of the system, which is determined by considering the topology of the grid. Let $|\mathcal{C}_b|$ be the cardinality of $\mathcal{C}_b$, then the *expected capacity* of the infrastructure is the expected number of surviving core components of the infrastructure given by

$$N_I = \sum_{b=1}^{N_b} |\mathcal{C}_b| \mathcal{P}_b.$$

Based on Theorem 5.1 (Eq. 11), the expected capacity of the infrastructure is defined as [4]

$$\hat{N}_I = \sum_{b=1}^{N_b} \frac{|\mathcal{C}_b| \left(\Delta_{\prod_b} \frac{\partial C_b}{\partial p_{c_{b,k}}} + \frac{\partial C_{\Delta_i}}{\partial p_{c_{b,k}}} + \frac{F^{D,b}_{G,L}}{L^D_{G,L}} \right)}{\Delta_{\prod_b} \frac{\partial C_b}{\partial p_{c_{b,k}}} - \left(1 - C_{\prod_b}\right) \Lambda_b}.$$

For basic systems which do not have the core resources, their effects on the expected capacity of the infrastructure are captured by various forms of correlation functions in the formula.

B. Upper Bound on the Survival Probability

Theorem 5.2: Under Condition 3.1 and Lemma 5.1, an upper bound on the survival probability of the basic system S_b at the Nash equilibrium is

$$\mathcal{P}_I(S_b) < 1 + \frac{\left(L^D_{G,L} \frac{\partial^2 \mathcal{P}_I(\mathcal{S})}{\partial p^2_{c_{b,k}}} + \frac{\partial F^{D,b}_{G,L}}{\partial p_{c_{b,k}}} \right)}{\Delta_{\prod_b} \frac{\partial L^D_{G,L}}{\partial p_{c_{b,k}}} \frac{\partial C_b}{\partial p_{c_{b,k}}}} + \left[(1 - C_{\prod_b}) \frac{\partial \mathcal{P}_I(S_b)}{\partial p_{c_{b,k}}} + \frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}} \right] \frac{1}{\Delta_{\prod_b} \frac{\partial C_b}{\partial p_{c_{b,k}}}},$$

where $k = 1, 2, \ldots, n_b$.

Proof: At NE, the first derivative of the utility function (Eq. 1) is given by

$$\frac{\partial U_D}{\partial p_{c_{b,k}}} = \left(G_D \frac{\partial F_{D,G}}{\partial \mathcal{P}_I(\mathcal{S})} + L_D \frac{\partial F_{D,L}}{\partial \mathcal{P}_I(\mathcal{S})} \right) \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} + F_{D,G} \frac{\partial G_D}{\partial p_{c_{b,k}}} + F_{D,L} \frac{\partial L_D}{\partial p_{c_{b,k}}} = L^D_{G,L} \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} + F^{D,b}_{G,L},$$

for $b = 1, 2, \ldots, N_{\mathcal{S}}$. The second derivative condition is given by

$$\frac{\partial^2 U_D}{\partial p^2_{c_{b,k}}} = L^D_{G,L} \frac{\partial^2 \mathcal{P}_I(\mathcal{S})}{\partial p^2_{c_{b,k}}} + \frac{\partial L^D_{G,L}}{\partial p_{c_{b,k}}} \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} + \frac{\partial F^{D,b}_{G,L}}{\partial p_{c_{b,k}}} > 0,$$

which in turn provides a bound on $\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}}$ as follows,

$$\frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial p_{c_{b,k}}} > - \left(L^D_{G,L} \frac{\partial^2 \mathcal{P}_I(\mathcal{S})}{\partial p^2_{c_{b,k}}} + \frac{\partial F^{D,b}_{G,L}}{\partial p_{c_{b,k}}} \right) \Bigg/ \frac{\partial L^D_{G,L}}{\partial p_{c_{b,k}}}.$$

The upper bound on $\mathcal{P}_I(S_b)$ then follows from Part (i) of Lemma 5.1. □

This theorem indicates that the product aggregate correlation function $C_{\prod_b}$, the partial derivative of the local aggregate failure correlation function $\frac{\partial C_b}{\partial p_{c_{b,k}}}$, and $\Delta_{\prod_b}$ could limit the achievable $\mathcal{P}_I(S_b)$. On the other hand, the achievable $\mathcal{P}_I(S_b)$ at NE can be improved by the cost term $L^D_{G,L}$, and the partial derivatives $\frac{\partial F^{D,b}_{G,L}}{\partial p_{c_{b,k}}}$ and $\frac{\partial C_{\Delta_b}}{\partial p_{c_{b,k}}}$.

VI. Application Examples

We now describe simple models of distributed cloud servers infrastructure, 5G network infrastructure, HPC federation, and smart energy grid infrastructure, and discuss the implications of analytical results derived in the previous section [2].

A. Distributed Cloud Servers Infrastructure

A cloud infrastructure consists of a variety of hardware and software components that are subject to a broad spectrum of attacks and risks, as reflected in the taxonomy in [2]. A distributed cloud servers infrastructure consists of N_F server sites and a user account management system is shown in Fig. 2. Cloud server infrastructures have been modeled using two-level and RSoS models under game formulation using the number of components, instead of the probability of reinforcement and attack on the components, in [60] and [1] respectively. Here, we focus on the component-based game formulation and consider additional software related details in terms of virtual machines and user accounts.

Server sites are connected over a wide-area network which is not explicitly modeled as we assume the wide-area network is not maintained by the provider. At site j, $j = 1, 2, \ldots, N_F$, there are one virtual machine manager, L_j server computers, some routers to connect the computers, some links to connect

[2]Related literature in each of these application areas is extensive, and we only refer to a few examples to contrast them from our hierarchical infrastructure model and the correlations-based game formulation.

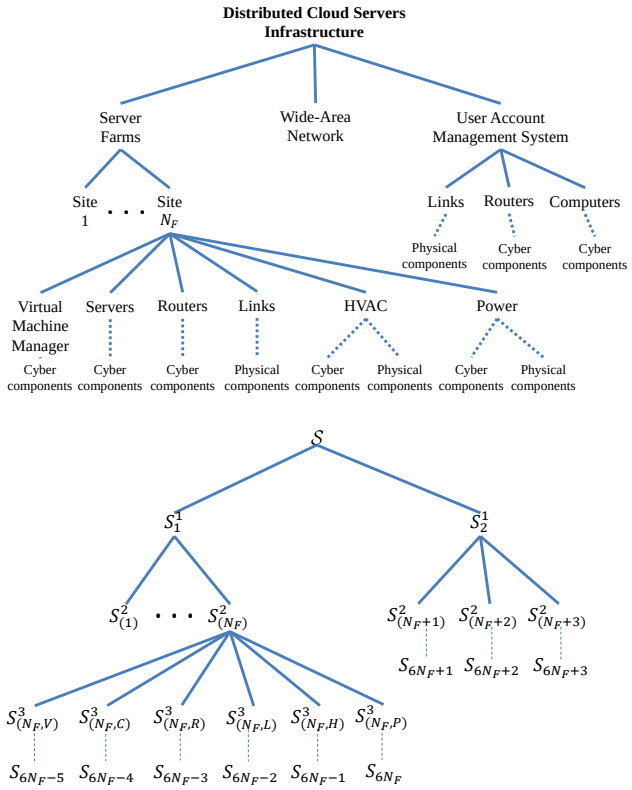


Fig. 2. RSoS tree representation of a distributed cloud servers infrastructure.

the site to the Internet, one Heating, Ventilation and Air-Conditioning (HVAC) system, and one power system. The virtual machine manager, servers, routers, HVAC, and power can be brought down by cyber attacks, and the links, HVAC, and power can be brought down by physical attacks. Meanwhile, the user account management system (UAMS) consists of links to the Internet, routers and also $L_{(U,C)}$ computers. The routers and computers can be brought offline by cyber attacks, while the links can be brought down by physical attacks. To reinforce the components of this infrastructure, redundant components can be deployed, for example, by replicating the servers and routers, and installing redundant fiber lines.

This infrastructure is modeled using $6N_F+3$ basic systems, i.e., $N_{\mathcal{S}} = 6N_F + 3$. At level 2, there are three basic systems, $S^2_{(N_F+1)}$, $S^2_{(N_F+2)}$, and $S^2_{(N_F+3)}$, which represent the links, routers, and computers of the user account management system, respectively. At level 3, there are $6N_F$ basic systems, where $S^3_{(j,V)}$, $S^3_{(j,C)}$, $S^3_{(j,R)}$, $S^3_{(j,L)}$, $S^3_{(j,H)}$, and $S^3_{(j,P)}$ represent the virtual machine manager, server computers, routers, links, HVAC, and power of site j, respectively. Thus, in terms of the original indices, the basic systems can be identified as follows:

(i) *virtual machine manager at a site:* $S_{6j-5} = S^3_{(j,V)}$, for $j = 1, 2, \ldots, N_F$,
(ii) *server computers at a site:* $S_{6j-4} = S^3_{(j,C)}$, for $j = 1, 2, \ldots, N_F$,
(iii) *routers at a site:* $S_{6j-3} = S^3_{(j,R)}$, for $j = 1, 2, \ldots, N_F$,
(iv) *links at a site:* $S_{6j-2} = S^3_{(j,L)}$, for $j = 1, 2, \ldots, N_F$,
(v) *HVAC at a site:* $S_{6j-1} = S^3_{(j,H)}$, for $j = 1, 2, \ldots, N_F$,
(vi) *power at a site:* $S_{6j} = S^3_{(j,P)}$, for $j = 1, 2, \ldots, N_F$,
(vii) *links at UAMS:* $S_{6N_F+1} = S^2_{(N_F+1)}$,
(viii) *routers at UAMS:* $S_{6N_F+2} = S^2_{(N_F+2)}$, and
(ix) *computers at UAMS:* $S_{6N_F+3} = S^2_{(N_F+3)}$.

The relationships between the local aggregate failure correlation functions provide useful insights (as described in [4]), and some of them are listed as follows. For the user account management system, we have

$$C^2_{(N_F+2)} = L_{(U,C)} C^2_{(N_F+1)}$$

which reflects that a successful router attack will disrupt all its $L_{(U,C)}$ connected management computers. (Similarly, a successful link attack will also disrupt its connected management computers.) For the sites, we have $C^3_{(j,L)} = L_j C^3_{(j,C)}$ which indicates that at site j, the fiber disruption will disconnect all its servers. (Similarly, if a virtual machine manager attack, a router attack, a HVAC attack, or a power supply attack is successful, it will also disrupt the operation of the servers at a site.) This multiplicative effect carries over to partial differentials since $\frac{\partial C^3_{(j,L)}}{\partial \mathcal{P}^3_{(j,C)}} = L_j \frac{\partial C^3_{(j,C)}}{\partial \mathcal{P}^3_{(j,C)}}$ and $\frac{\partial C^3_{(j,L)}}{\partial \mathcal{P}^3_{(j,L)}} = L_j \frac{\partial C^3_{(j,C)}}{\partial \mathcal{P}^3_{(j,L)}}$ for $j = 1, 2, \ldots, N_F$, and $\frac{\partial C^2_{(N_F+2)}}{\partial \mathcal{P}^2_{(N_F+3)}} = L_{(U,C)} \frac{\partial C^2_{(N_F+3)}}{\partial \mathcal{P}^2_{(N_F+3)}}$ and $\frac{\partial C^2_{(N_F+2)}}{\partial \mathcal{P}^2_{(N_F+2)}} = L_{(U,C)} \frac{\partial C^2_{(N_F+3)}}{\partial \mathcal{P}^2_{(N_F+2)}}$. Based on Theorem 5.1, this multiplicative effect in partial differentials will be reflected in $\hat{\mathcal{P}}_{(j,L);D}$ and $\hat{\mathcal{P}}_{-(j,L);D}$ in addition to the correlations.

Now consider three basic systems $S_{b_1} = S_{6j-4} = S^3_{(j,C)}$ and $S_{b_2} = S_{6j-2} = S^3_{(j,L)}$ corresponding to the collections of servers and fibers of site j, respectively, and $S_{b_3} = S_{6N_F+1} = S^2_{(N_F+1)}$ corresponding to the links of the user account management system. Then, the product multiplier function (Eq. 9) of S_{b_3} is

$$\Lambda_{\prod_{b_3}} = \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial \mathcal{P}_I(S^1_2)} \frac{\partial \mathcal{P}_I(S^1_2)}{\partial \mathcal{P}_I\left(S^2_{(N_F+1)}\right)} \Lambda_{b_3}.$$

That of the collection of servers S_{b_1} of site j is

$$\Lambda_{\prod_{b_1}} = \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial \mathcal{P}_I(S^1_1)} \frac{\partial \mathcal{P}_I(S^1_1)}{\partial \mathcal{P}_I\left(S^2_{(j)}\right)} \frac{\partial \mathcal{P}_I\left(S^2_{(j)}\right)}{\partial \mathcal{P}_I\left(S^3_{(j,C)}\right)} \Lambda_{b_1},$$

which is more complex since S_{b_1} is at a deeper level. Similarly, the product aggregate correlation function (Eq. 8) of S_{b_3} given by

$$C_{\prod_{b_3}} = 1 - (1 - C^1_2)\left(1 - C^2_{(N_F+1)}\right)$$

is simpler than those of S_{b_1} and S_{b_2} given by

$$C_{\prod_{b_1}} = 1 - (1 - C^1_1)\left(1 - C^2_{(j)}\right)(1 - C_{b_1}),$$

$$C_{\prod_{b_2}} = 1 - (1 - C^1_1)\left(1 - C^2_{(j)}\right)(1 - C_{b_2}).$$

Here $C_{b_1} = C_{(j,C)} \approx 0$ since failure of servers does not lead to that of other systems and $C_{b_2} = C_{(j,L)} \approx 1$ since the failure of fibers will render other systems unavailable. Consequently, the product term $\left(1 - C_{\prod_{b_1}}\right)\Lambda_{b_1}$ in Theorem 5.1 indicates higher sensitivity of the servers compared to $\left(1 - C_{\prod_{b_2}}\right)\Lambda_{b_2}$ of the fibers. Note that the two product aggregate correlation functions, $C_{\prod_{b_2}}$ and $C_{\prod_{b_3}}$, are related: (i) C^1_2 relates the

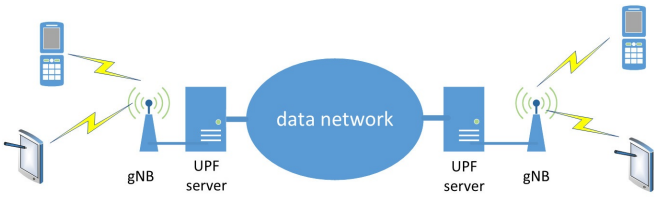


Fig. 3. A 5G network infrastructure.

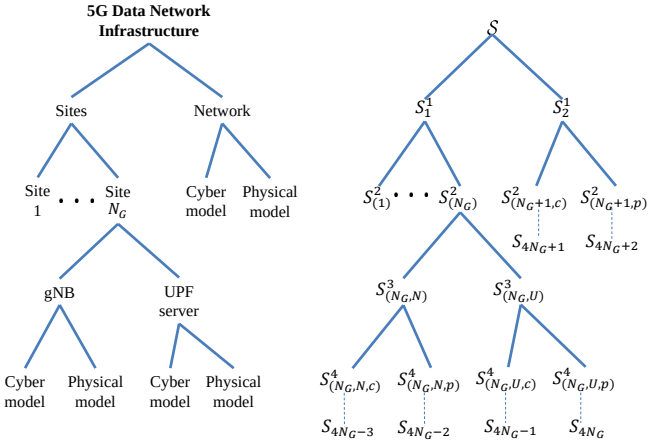


Fig. 4. RSoS tree representation of a 5G network infrastructure.

user account management system S_2^1 to $\mathcal{S}^1_{-S_2^1}$ that subsume $S^2_{(N_F+1)}$ and $S^3_{(j,L)}$, respectively, and (ii) C_1^1 relates the server farm S_1^1 to $\mathcal{S}^1_{-S_1^1}$, which is the user account management system S_2^1, that subsume the site $S^2_{(j)}$ and the link $S^2_{(N_F+1)}$, respectively, and $S^2_{(j)}$ further subsumes $S^3_{(j,L)}$.

The expected capacity of this infrastructure can be specified by the expected number of surviving servers given by $N_I = \sum_{j=1}^{N_F} c_j \mathcal{P}_{6j-4}$, where c_j is the number of servers of the system S_{6j-4} at site j.

B. 5G Network Infrastructure

Recent advances in 5G networking support the provisioning of end-to-end connections between mobile devices with specified Quality of Service (QoS) parameters over a data network using User Plane Functions (UPF) capabilities. This infrastructure and the supported mobile applications are subject to a variety of security threats [73], [74]. In particular, this infrastructure is supported by UPF servers that connect wireless base stations (gNB) to the data network to provide services that complement voice and other services, as shown in Fig. 3, and is also vulnerable to various types of attacks [73]. Here, a gNB serves 5G devices which are within its range, and supports their connections over data network via a UPF server. The RSoS model of a 5G network is shown in Fig. 4. This infrastructure spans N_G sites, $S_1^2, S_2^2, \ldots, S_{N_G}^2$, each with a dedicated gNB and a UPF server. The data network is similar to the network in a cloud servers infrastructure and is represented by its cyber and physical models, denoted by $S^2_{(N_G+1,c)}$ and $S^2_{(N_G+1,p)}$, respectively, and can be further expanded as described in Section VI-A.

The gNB of site i is represented by $S^3_{(i,N)}$ at level 3, and is refined into its cyber model $S^4_{(i,N,c)}$ that captures its cyber attacks, such as infection of malware or malicious firmware, and physical model $S^4_{(i,N,p)}$ that captures the physical attacks, such as physical damage and power disruption, on the cell tower which is typically in an open area. Its UPF server is represented by $S^3_{(i,U)}$ at level 3, and is refined into its cyber model $S^4_{(i,U,c)}$ that captures its cyber attacks, such as malware infection, and physical model $S^4_{(i,U,p)}$ that captures the physical attacks and damages on the fiber connecting it to the gNB. Unlike the gNB which is often in an open area, the UPF server is typically housed inside a facility which is not subject to physical disruption but its fiber connection is still in the open. Reinforcement of the components in such an infrastructure involves deploying redundant servers and fiber connections. Thus, in terms of the original indices, the basic systems can be identified as follows:

(i) *cyber model of wireless base station gNB at a site:* $S_{4j-3} = S^4_{(j,N,c)}$, for $j = 1, 2, \ldots, N_G$,
(ii) *physical model of wireless base station gNB at a site:* $S_{4j-2} = S^4_{(j,N,p)}$, for $j = 1, 2, \ldots, N_G$,
(iii) *cyber model of data network UPF server at a site:* $S_{4j-1} = S^4_{(j,U,c)}$, for $j = 1, 2, \ldots, N_G$,
(iv) *physical model of data network UPF server at a site:* $S_{4j} = S^4_{(j,U,p)}$, for $j = 1, 2, \ldots, N_G$,
(v) *cyber model of the data network:* $S_{4N_G+1} = S^2_{(N_G+1,c)}$, and
(vi) *physical model of the data network:* $S_{4N_G+2} = S^2_{(N_G+1,p)}$.

For the sites, we have $C^3_{(j,U)} = C^3_{(j,N)}$ which indicates that at site j, the UPF server disruption will disconnect the wireless base station gNB. This effect carries over to partial differentials since $\frac{\partial C^3_{(j,U)}}{\partial \mathcal{P}^3_{(j,N)}} = \frac{\partial C^3_{(j,N)}}{\partial \mathcal{P}^3_{(j,N)}}$ and $\frac{\partial C^3_{(j,U)}}{\partial \mathcal{P}^3_{(j,U)}} = \frac{\partial C^3_{(j,N)}}{\partial \mathcal{P}^3_{(j,U)}}$ for $j = 1, 2, \ldots, N_G$. Based on Theorem 5.1, this effect in partial differentials will be reflected in $\hat{\mathcal{P}}_{(j,U);D}$ and $\hat{\mathcal{P}}_{-(j,U);D}$ in addition to the correlations.

Now consider two basic systems $S_{b_1} = S_{4j-3} = S^4_{(j,N,c)}$ corresponding to the cyber model of gNB at site j and $S_{b_2} = S_{4N_G+2} = S^2_{(N_G+1,p)}$ corresponding to the physical model of the data network. Then, the product multiplier function (Eq. 9) of S_{b_2} is

$$\Lambda_{\prod_{b_2}} = \frac{\partial P_I(\mathcal{S})}{\partial P_I(S_2^1)} \frac{\partial P_I(S_2^1)}{\partial P_I\left(S^2_{(N_G+1,p)}\right)} \Lambda_{b_2}.$$

That of the cyber model of gNB at site j, S_{b_1}, is

$$\Lambda_{\prod_{b_1}} = \frac{\partial P_I(\mathcal{S})}{\partial P_I(S_1^1)} \frac{\partial P_I(S_1^1)}{\partial P_I\left(S^2_{(j)}\right)} \frac{\partial P_I\left(S^2_{(j)}\right)}{\partial P_I\left(S^3_{(j,N)}\right)} \frac{\partial P_I\left(S^3_{(j,N)}\right)}{\partial P_I\left(S^4_{(j,N,c)}\right)} \Lambda_{b_1},$$

which is more complex since S_{b_1} is at a deeper level. Similarly, the product aggregate correlation function (Eq. 8) of S_{b_2} given by

$$C_{\prod_{b_2}} = 1 - \left(1 - C_2^1\right)\left(1 - C_{b_2}\right)$$

is simpler than that of S_{b_1} given by

$$C_{\prod_{b_1}} = 1 - \left(1 - C_1^1\right)\left(1 - C^2_{(j)}\right)\left(1 - C^3_{(j,N)}\right)\left(1 - C_{b_1}\right).$$

Note that these two product aggregate correlation functions are related: (i) C_2^1 relates the network system S_2^1 to $\mathcal{S}^1_{-S_2^1}$

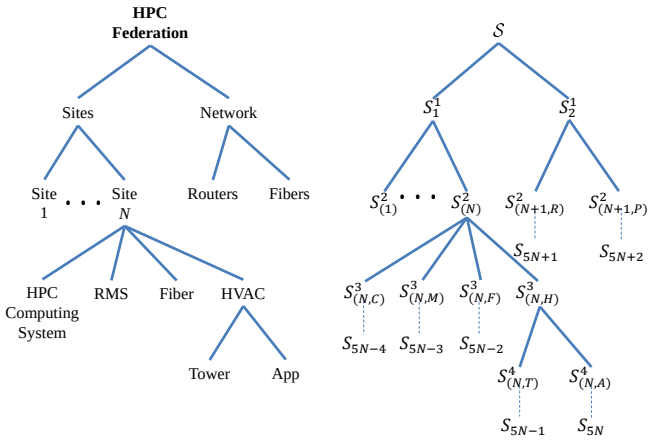


Fig. 5. RSoS tree representation of a HPC federation.

that subsume $S^2_{(N_G+1,p)}$ and $S^4_{(j,N,c)}$, respectively, and (ii) C^1_1 relates the site $S^2_{(j)}$ to $\mathcal{S}^2_{-S^2_{(j)}}$ that subsume $S^4_{(j,N,c)}$ and $S^2_{(N_G+1,p)}$, respectively.

The expected capacity of this 5G data network can be specified in terms of the expected number of surviving gNB given by $N_I = \sum_{j=1}^{N_G} b_j \mathcal{P}_{4j-3}$ where b_j is the capacity of gNB, S_{4j-3}, at site j. Here, the capacity b_j can be defined various ways, including the number of mobile users supported, their aggregate data network capacity and others; in particular, for $b_j = 1$, N_I/N_G represents the fraction of the coverage area served by the surviving gNB.

C. HPC Federation

A generic HPC federation with N geographically distributed sites [75] connected over a wide-area communications network is illustrated in Fig. 5. Each site houses a supercomputer of potentially different size and architecture, a Resource Management System (RMS), and its HVAC system consists of cooling towers and an app that controls its temperature settings. HPC federation can be modeled using RSoS, and its game formulation based on the number of components has been discussed in detail in [61]. In this section, we focus on the component-based formulation with the additional details of RMS.

Cyber attacks on the computing system, RMS, and HVAC control app (typically on a phone or tablet) can bring down the computing system in different ways; for example, the first may crash the computing system, the second may disable the computing system, and the last may manipulate the app to increase the temperature to trigger a system shutdown. Physical damages to the HVAC cooling tower can lead to a computing system shutdown, and cuts of communication fibers can render the computing system unavailable over the networks; these disruptions may be carried out at locations outside the building housing the computing system. Meanwhile, the wide-area communications network connects the sites, and each of its routers manages more than one fiber connection. Let router i manage L_i connections, a successful cyber attack on the router will disconnect all its connections, i.e., the L_i sites, whereas a fiber attack may disconnect one or some of them. To reinforce the components of this infrastructure, some nodes of supercomputers and routers may be replicated, and redundant fiber lines may be installed.

Each site is modeled at a coarse level by five basic systems as shown in Fig. 5, namely a HPC computing system, RMS, site fiber connections, HVAC cooling towers and its app, which can be structured as a sub-tree. As systems, a site and a network are structurally quite different and consist of different types of components, namely, computing and communications devices, respectively. This infrastructure is modeled at a coarse level by a RSoS consisting of $N+2$ systems at level 2, where $S^2_{(N+1,R)}$ and $S^2_{(N+1,P)}$ represent the routers and fiber lines of the communications network as illustrated in Fig. 5. At level 3, there are $4N$ systems where $S^3_{(j,C)}$, $S^3_{(j,M)}$, $S^3_{(j,F)}$, and $S^3_{(j,H)}$ represent the computing system, RMS, fiber connections, and HVAC system of site j, respectively. At level 4, for each site j we have the cooling towers represented by $S^4_{(j,T)}$ and HVAC control app represented by $S^4_{(j,A)}$. Thus, in terms of the original indices, the basic systems at a coarse level can be identified as follows:

(i) *HPC computing systems:* $S_{5j-4} = S^3_{(j,C)}$, for $j = 1, 2, \ldots, N$,
(ii) *RMS:* $S_{5j-3} = S^3_{(j,M)}$, for $j = 1, 2, \ldots, N$,
(iii) *site fiber connections:* $S_{5j-2} = S^3_{(j,F)}$, for $j = 1, 2, \ldots, N$,
(iv) *HVAC system cooling towers and control App:* $S_{5j-1} = S^4_{(j,T)}$, $S_{5j} = S^4_{(j,A)}$ for $j = 1, 2, \ldots, N$, and
(v) *wide-area network with routers and physical connections:* $S_{5N+1} = S^2_{(N+1,R)}$ and $S_{5N+2} = S^2_{(N+1,P)}$.

Thus, there are $N_{\mathcal{S}} = 5N+2$ basic systems that constitute the leaves of the RSoS tree, which correspond to the two basic systems at level 2, $3N$ basic systems at level 3, and $2N$ basic systems at level 4.

For the sites, we have $C^3_{(j,F)} = C^3_{(j,C)}$ which indicates that at site j the fiber disruption will disconnect the HPC computing system. This effect carries over to partial differentials since $\frac{\partial C^3_{(j,F)}}{\partial \mathcal{P}^3_{(j,C)}} = \frac{\partial C^3_{(j,C)}}{\partial \mathcal{P}^3_{(j,C)}}$ and $\frac{\partial C^3_{(j,F)}}{\partial \mathcal{P}^3_{(j,F)}} = \frac{\partial C^3_{(j,C)}}{\partial \mathcal{P}^3_{(j,F)}}$ for $j = 1, 2, \ldots, N$. Based on Theorem 5.1, this effect in partial differentials will be reflected in $\hat{\mathcal{P}}_{(j,F);D}$ and $\hat{\mathcal{P}}_{-(j,F);D}$ in addition to the correlations. Similarly, we have $C^3_{(j,M)} = C^3_{(j,C)}$ which indicates that at site j, the RMS disruption will also disconnect the HPC computing system, and this effect also carries over to partial differentials.

Now consider two basic systems $S_{b_1} = S_{4j} = S^4_{(j,A)}$ corresponding to the HVAC app of site j and $S_{b_2} = S_{4N+2} = S^2_{(N+1,P)}$ corresponding to the fiber lines of the communications network. Then, the product multiplier function (Eq. 9) of S_{b_2} is

$$\Lambda_{\prod_{b_2}} = \frac{\partial P_I(\mathcal{S})}{\partial P_I(S^1_2)} \frac{\partial P_I(S^1_2)}{\partial P_I\left(S^2_{(N+1,P)}\right)} \Lambda_{b_2}.$$

That of the HVAC app of site j, S_{b_1}, is

$$\Lambda_{\prod_{b_1}} = \frac{\partial P_I(\mathcal{S})}{\partial P_I(S^1_1)} \frac{\partial P_I(S^1_1)}{\partial P_I\left(S^2_{(j)}\right)} \frac{\partial P_I\left(S^2_{(j)}\right)}{\partial P_I\left(S^3_{(j,H)}\right)} \frac{\partial P_I\left(S^3_{(j,H)}\right)}{\partial P_I\left(S^4_{(j,A)}\right)} \Lambda_{b_1},$$

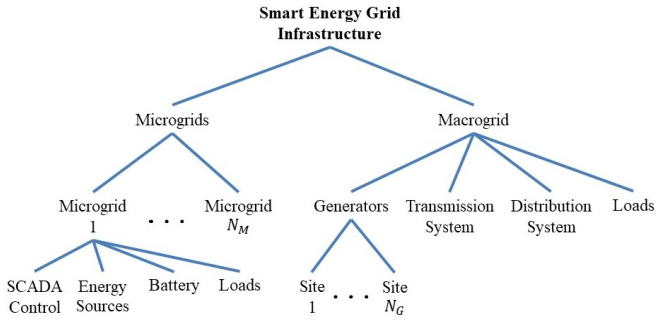


Fig. 6. Representation of a smart energy grid infrastructure.

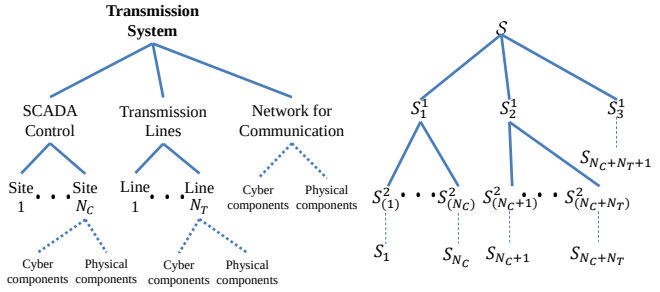


Fig. 7. RSoS tree representation of a transmission system in the macrogrid.

which is more complex since S_{b_1} is at a deeper level. Similarly, the product aggregate correlation function (Eq. 8) of S_{b_2} given by

$$C_{\prod_{b_2}} = 1 - \left(1 - C_2^1\right)\left(1 - C_{b_2}\right)$$

is simpler than that of HVAC app of site j, S_{b_1}, given by

$$C_{\prod_{b_1}} = 1 - \left(1 - C_1^1\right)\left(1 - C_{(j)}^2\right)\left(1 - C_{(j,H)}^3\right)\left(1 - C_{b_1}\right).$$

Note that these two product aggregate correlation functions are related: (i) C_2^1 relates the network system S_2^1 to $\mathcal{S}_{-S_2^1}^1$ that subsume $S_{(N+1,P)}^2$ and $S_{(j,A)}^4$, respectively, and (ii) C_1^1 relates the site $S_{(j)}^2$ to $\mathcal{S}_{-S_{(j)}^2}^2$ that subsume $S_{(j,A)}^4$ and $S_{(N+1,P)}^2$, respectively. Here, $C_{b_1} \approx 1$ since the failure of HVAC app at site j renders its computing system unavailable, and $C_{b_2} \approx 1$ since failures of all fibers in the wide-area network render all computing systems unavailable, which in turn lead to $C_{\prod_{b_2}} \approx 1$; consequently both $C_{\prod_{b_1}}$ and $C_{\prod_{b_2}}$ approach 1.

Let c_j and g_j represent the number of CPU and GPU processor cores, respectively, at the computing system S_{4j-3} at site j. The expected capacity of this HPC federation can be specified by the expected number of surviving processor cores given by $N_I = \sum_{j=1}^{N}(c_j + g_j)\mathcal{P}_{4j-3}$.

D. Smart Energy Grid Infrastructure

A smart grid infrastructure may consist of a macrogrid that provides stable long-term energy sources, which complements a collection of smaller-scale, dynamic microgrids [17], [76]. Typically, a microgrid consists of renewable power generators such as solar panels and wind turbines, smart meters and energy storage devices such as batteries, to support small systems such as homes and offices. A game theoretic formulation of a microgrid infrastructure has been studied using the prospect theory in [77], which can be viewed to constitute a single-level RSoS model. We consider a simplified model of a smart energy grid infrastructure as shown in Fig. 6, which consists of one macrogrid and N_M microgrids. It is an expanded version of a much simpler two-level model of a smart power grid studied in [5]. For simplicity, we focus only on the transmission system of the macrogrid as shown in Fig. 7, which is a main part of the smart energy grid infrastructure; the microgrids can be similarly analyzed. The transmission system is controlled by N_C Supervisory Control and Data Acquisition (SCADA) sites, such that site j controls the power flow on L_j transmission lines, for $j = 1, 2, \ldots, N_C$. The SCADA system of site j may become non-operational due to a direct cyber or physical attack, which in turn will disrupt power flow on all its L_j lines. The SCADA systems are connected to a communications network. Hence, the SCADA system of site j may also become non-operational due to a direct cyber or physical attack of the communications network. A transmission line may also become non-operational due to a direct cyber or physical attack.

This transmission system is modeled using $N_C + N_T + 1$ basic systems, i.e., $N_{\mathcal{S}} = N_C + N_T + 1$. At level 1, there is one basic system, S_3^1, which represents the communications network. At level 2, there are $N_C + N_T$ basic systems, where $S_{(j)}^2$, $j = 1, 2, ..., N_C$, represent the model of SCADA sites and $S_{(N_C+j)}^2$, $j = 1, 2, ..., N_T$, represent the transmission lines. Thus, in terms of the original indices, the basic systems can be identified as follows:

(i) *SCADA site model:* $S_j = S_{(j)}^2$, for $j = 1, 2, \ldots, N_C$,
(ii) *transmission line model:* $S_{N_C+j} = S_{(N_C+j)}^2$, for $j = 1, 2, \ldots, N_T$, and
(iii) *network model:* $S_{N_C+N_T+1} = S_3^1$.

For this transmission system, we have $C_{(j)}^2 = L_j C_{(N_C+m)}^2$, for $j = 1, 2, \ldots, N_C$ and $m = 1, 2, \ldots, N_T$, since a successful cyber attack on the SCADA system at site j would disrupt the power flow on all L_j lines. Similarly, a successful communications network attack would also disrupt the power flow on all transmission lines by disrupting the communication between the transmission lines and SCADA systems, i.e., we have $C_3^1 = N_C C_{(j)}^2 = N_C \times L_j C_{(m)}^2 = N_T C_{(N_C+m)}^2$, for $j = 1, 2, \ldots, N_C$ and $m = 1, 2, \ldots, N_T$. Also, these multiplicative effects will be reflected in the corresponding partial derivatives, and in $\hat{\mathcal{P}}_{i;D}$ and $\hat{\mathcal{P}}_{-i;D}$, for $i = 1, 2, \ldots, (N_C + N_T + 1)$.

Now consider two basic systems $S_{b_1} = S_3^1$ corresponding to the communications network and $S_{b_2} = S_{(N_C+1)}^2$ corresponding to a transmission line. Then, the product multiplier function (Eq. 9) of the communications network S_{b_1} is

$$\Lambda_{\prod_{b_1}} = \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial \mathcal{P}_I(S_3^1)} \Lambda_{b_1},$$

while that of the transmission line S_{b_2} is

$$\Lambda_{\prod_{b_2}} = \frac{\partial \mathcal{P}_I(\mathcal{S})}{\partial \mathcal{P}_I(S_2^1)} \frac{\partial \mathcal{P}_I(S_2^1)}{\partial \mathcal{P}_I\left(S_{(N_C+1)}^2\right)} \Lambda_{b_2},$$

which is more complex since S_{b_2} is at a deeper level. Similarly, the product aggregate correlation function (Eq. 8) of S_{b_1} given by

$$C_{\prod_{b_1}} = 1 - (1 - C_3^1) = C_{b_1}$$

is simpler than that of S_{b_2} given by

$$C_{\prod_{b_2}} = 1 - (1 - C_2^1)(1 - C_{b_2}).$$

Note that these two product aggregate correlation functions are related: (i) $C_{b_1} = C_3^1$ relates the communications network S_3^1 to $\mathcal{S}^1_{-S_3^1}$ which subsumes $S^2_{(N_C+1)}$, and (ii) C_2^1 relates the transmission line $S^2_{(N_C+1)}$ to $\mathcal{S}^2_{-S^2_{(N_C+1)}}$ which subsumes S_3^1.

Let f_j represent the capacity of flow in transmission line S_j, then the expected total flow in this infrastructure is given by $N_I = \sum_{j=1}^{N_T} f_j \mathcal{P}_{N_C+j}$. With suitable Boolean values assigned to f_j's, the number of the surviving microgrids and SCADA sites can be obtained.

VII. Conclusions

A class of infrastructures with recursively defined systems with discrete cyber and physical components are studied, under a game theoretic formulation with sum-of-products utility functions. Individual components of a system can be disrupted directly or indirectly by either by a cyber or physical attack. The components may be reinforced against such attacks by explicitly taking into account the correlations between the systems and also between the components within individual systems. The interactions between the systems in these infrastructures are characterized using the aggregate correlation functions, and those between the components within a system are characterized by the system multiplier functions; both functions can be estimated from observations or measurements, or analytically modeled in practical scenarios. By formulating a game between an infrastructure provider and an attacker, we derived the Nash Equilibrium conditions in terms of the partial derivatives of cost terms, aggregate correlation functions and survival probabilities of component systems and their partial derivatives. We then estimated the sensitivity functions that indicate the dependence of the system survival probability on these quantities.

These results address the attacks and reinforcements of individual components, and thus extend the previous results that model interactions using the number of components attacked and reinforced in each basic system [1], [4]. In particular, these results enable us to derive cost-centric strategies using simple models of distributed cloud servers, 5G data networks, high performance computing federations, and smart energy grid infrastructures.

Several extensions of the formulation studied in this paper can be pursued in future studies. It would be interesting to study the sequential game formulations of this problem [78], and cases where different levels and types of knowledge are available to attackers and providers, including, misinformation, persistent threats and subjective attacker priorities. Another research direction is to include explicit models for the survival of systems [79] and their interdependencies [57], and subjective decision making using the prospect theory [3], [6]. Applications of our approach to more detailed models of distributed cloud servers infrastructure, 5G data network infrastructures, high performance computing federations, smart energy grid infrastructures, and other infrastructures (such as metro systems [5]) would be of future interest. In several infrastructures, the wide-area networks play a dual, often conflicting, role in providing the critical accessibility to services and also as potential conduits for cyber attacks; it would be of future interest to develop formulations that explicitly reflect these aspects. It would also be of future interest to explore the applicability of this overall method to infrastructures characterized by continuous models such as partial differential equations describing the individual systems or the entire infrastructure, for example, transportation systems [80].

Acknowledgments

The authors acknowledge the constructive feedback from the anonymous reviewers that significantly improved the presentation and references to related works in this paper. This work is funded by RAMSES and Cyber-Physical Networks projects, Office of Advanced Computing Research, U.S. Department of Energy, and by Extreme Scale Systems Center, sponsored by U.S. Department of Defense, and performed at Oak Ridge National Laboratory managed by UT-Battelle, LLC for U.S. Department of Energy under Contract No. DE-AC05-00OR22725; and partially supported by grant UGC/FDS14/E01/19 from the Research Grants Council of the Hong Kong Special Administrative Region and the Deep Learning and Cognitive Computing Centre in The Hang Seng University of Hong Kong.

References

[1] N. S. V. Rao, C. Y. T. Ma, and F. He, "On defense strategies for recursive system of systems using aggregated correlations," in *International Conference on Information Fusion*, 2018.

[2] N. V. Juliadotter and K.-K. R. Choo, "Cloud attack and risk assessment taxonomy," *IEEE Cloud Computing*, vol. 2, no. 1, pp. 14–20, 2015.

[3] L. Xiao, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, "Cloud storage defense against advanced persistent threats: A prospect theoretic study," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 534–544, 2017.

[4] N. S. V. Rao, C. Y. T. Ma, K. Hausken, F. He, D. K. Y. Yau, and J. Zhuang, "Defense strategies for asymmetric networked systems with discrete components," *Sensors*, vol. 18, p. 1421, 2018.

[5] N. S. V. Rao, C. Y. T. Ma, F. He, D. K. Y. Yau, and J. Zhuang, "Cyberphysical correlation effects in defense games for large discrete infrastructures," *Games*, vol. 9, no. 52, 2018.

[6] L. Xiao, D. Xu, N. B. Mandayam, and H. V. Poor, "Attacker-centric view of a detection game against advanced persistent threats," *IEEE transactions on mobile computing*, vol. 17, no. 11, pp. 2512–2523, 2018.

[7] Y. Li, S. Qiao, Y. Deng, and J. Wu, "Stackelberg game in critical infrastructures from a network science perspective," *Physica A: Statistical Mechanics and its Applications*, vol. 521, pp. 705–714, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378437119301268

[8] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 2003.

[9] G. Brown, M. Carlyle, J. Salmern, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 532–544, 2006.

[10] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[11] T. G. Lewis, *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons, 2014.

[12] F. Pasqualetti, F. Drfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[13] A. Chattopadhyay, A. Prakash, and M. Shafique, "Secure cyber-physical systems: current trends, tools and open research problems," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*. IEEE, 2017, pp. 1104–1109.

[14] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems securitya survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[15] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," *Transactions on internet and information systems*, vol. 8, no. 12, pp. 4242–4268, 2014.

[16] S. C. Suh, U. J. Tanik, J. N. Carbone, and A. Eroglu, Eds., *Applied Cyber-Physical Systems*. Springer-Verlag, 2014.

[17] D. W. McKee, S. J. Clement, J. Almutairi, and J. Xu, "Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems," *CAAI Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 75–82, 2018.

[18] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *2014 IEEE world forum on internet of things (WF-IoT)*. IEEE, 2014, pp. 241–246.

[19] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan 2018.

[20] K. Hausken, "Defense and attack for interdependent systems," *European Journal of Operational Research*, vol. 256, pp. 582–591, 2016.

[21] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *The 28th International Conference on Distributed Computing Systems Workshops*. IEEE, 2008, pp. 495–500.

[22] J. Beyza, E. Garcia-Paricio, and J. M. Yusta, "Applying complex network theory to the vulnerability assessment of interdependent energy infrastructures," *Energies*, vol. 12, no. 3, p. 421, 2019.

[23] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: Structure and dynamics," *Physics reports*, vol. 424, no. 4-5, pp. 175–308, 2006.

[24] T. Alpcan and T. Basar, *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press, 2011.

[25] N. Ghorbani-Renani, A. D. González, K. Barker, and N. Morshedlou, "Protection-interdiction-restoration: Tri-level optimization for enhancing interdependent network resilience," *Reliability Engineering & System Safety*, vol. 199, p. 106907, 2020.

[26] N. S. V. Rao, Y. Narahari, C. E. V. Madhavan, D. K. Y. Yau, and C. Y. T. Ma, "An analytical framwork for cyber-physical networks," in *Securing Cyber-Physical Infrastructures: Foundations and Challenges*, S. K. Das, K. Kant, and N. Zhang, Eds. Morgan Kaufmann, 2012.

[27] V. M. Bier and M. N. Azaiez, Eds., *Game Theoretic Risk Analysis of Security Threats*. Springer, 2009.

[28] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 24–29, 2012.

[29] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, p. 25, 2013.

[30] S. Shiva, S. Roy, and D. Dasgupta, "Game theory for cyber security," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*. ACM, 2010, p. 34.

[31] R. Yu, Y. H. Chen, and B. Han, "Cooperative game approach to robust control design for fuzzy dynamical systems," *IEEE Transactions on Cybernetics*, pp. 1–13, 2020.

[32] J. Li, J. Ding, T. Chai, and F. L. Lewis, "Nonzero-sum game reinforcement learning for performance optimization in large-scale industrial processes," *IEEE Transactions on Cybernetics*, vol. 50, no. 9, pp. 4132–4145, 2020.

[33] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 46–65, 2015.

[34] A. Ferdowsi, A. Eldosouky, and W. Saad, "Interdependence-aware game-theoretic framework for secure intelligent transportation systems," *IEEE Internet of Things Journal*, 2020.

[35] D. Alderson, G. Brown, W. Carlyle, and R. Wood, "Solving defender-attacker-defender models for infrastructure defense," in *INFORMS Computing Society Conference*, 2011, pp. 28–49.

[36] Y. Li, S. Tan, Y. Deng, and J. Wu, "Attacker-defender game from a network science perspective," *Chaos*, vol. 28, no. 5, pp. 051 102–051 109, 2018.

[37] M. Ouyang, "A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks," *European J. Oper. Res.*, vol. 262, no. 3, pp. 1072–1084, 2017.

[38] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "Security games with unknown adversarial strategies," *IEEE Transactions on Cybernetics*, vol. 46, no. 10, pp. 2291–2299, 2016.

[39] V. R. R. Jose and J. Zhuang, "Technology adoption, accumulation, and competition in multi-period attacker-defender games," *Military Operations Research*, vol. 18, no. 2, pp. 33–47, 2013.

[40] D. Arce, D. Kovenock, and B. Roberson, "Weakest-link attacker-defender games with multiple attack technologies," *Naval Res. Logist.*, vol. 59, no. 6, pp. 457–469, 2012.

[41] F. He and J. Zhuang, "Modelling 'contracts' between a terrorist group and a government in a sequential game," *Journal of the Operational Research Society*, vol. 63, no. 6, pp. 790–809, 2012.

[42] M. Nikoofal and J. Zhuang, "Robust allocation of a defensive budget considering an attacker's private information," *Risk Analysis*, vol. 32, no. 5, pp. 930–943, 2012.

[43] C. Zhang, J. E. Ramirez-Marquez, and J. Wang, "Critical infrastructure protection using secrecy - a discrete simultaneous game," *European Journal of Operational Research*, vol. 242, no. 1, pp. 212–221, 2015.

[44] K. Hausken and F. He, "On the effectiveness of security countermeasures for critical infrastructures," *Risk Analysis*, vol. 36, no. 4, pp. 711–726, 2016.

[45] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordez, and M. Tambe, "Computing optimal randomized resource allocations for massive security games," in *Proc. of International Joint Conference on Autonomous Agents and Multiagent Systems*, vol. 2, Jan. 2009, pp. 689–696.

[46] D. Korzhyk, V. Conitzer, and R. Parr, "Complexity of computing optimal stackelberg strategies in security resource allocation games," in *Proc. of the AAAI Conference on Artificial Intelligence*, vol. 24, no. 1, 2010.

[47] Y. Li, S. Qiao, Y. Deng, and J. Wu, "Stackelberg game in critical infrastructures from a network science perspective," *Physica A: Statistical Mechanics and its Applications*, vol. 521, Feb. 2019.

[48] E. C. Paulson, I. Linkov, and J. M. Keisler, "A game theoretic model for resource allocation among countermeasures with multiple attributes," *European Journal of Operational Research*, vol. 252, no. 2, pp. 610–622, 2016.

[49] X. Shan and J. Zhuang, "Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender-attacker game," *European Journal of Operational Research*, vol. 228, no. 1, pp. 262–272, 2013.

[50] Y. Mei, W. Han, S. Li, and X. Wu, "A survey of advanced persistent threats attack and defense," in *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*. Los Alamitos, CA, USA: IEEE Computer Society, oct 2021, pp. 608–613. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/DSC53577.2021.00096

[51] K. Hausken and G. Levitin, "Review of systems defense and attack models," *International Journal of Performability Engineering*, vol. 8, no. 4, pp. 355–366, 2012.

[52] I. Atzeni, L. G. Ordóñez, G. Scutari, D. P. Palomar, and J. R. Fonollosa, "Noncooperative and cooperative optimization of distributed energy generation and storage in the demand-side of the smart grid," *IEEE transactions on signal processing*, vol. 61, no. 10, pp. 2454–2472, 2013.

[53] T. G. Alghamdi, D. Said, and H. T. Mouftah, "Decentralized game-theoretic scheme for d-evse based on renewable energy in smart cities: A realistic scenario," *IEEE Access*, vol. 8, pp. 48 274–48 284, 2020.

[54] P. Shakarian, H. Lei, and R. Lindelauf, "Power grid defense against malicious cascading failure," in *Proc. of the international conference on Autonomous Agents and Multi-Agent Systems*, 2014, pp. 813–820.

[55] Q. Dai, X. Xu, W. Guo, S. Huang, and D. Filev, "Towards a systematic computational framework for modeling multi-agent decision-making at micro level for smart vehicles in a smart world," *Robotics and Autonomous Systems*, vol. 144, p. 103859, 2021.

[56] R. Aringhieri, M. E. Bruni, S. Khodaparasti, and J. T. van Essen, "Emergency medical services and beyond: Addressing new challenges through a wide literature review," *Computers & Operations Research*, vol. 78, pp. 349–368, 2017.

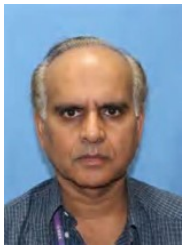
[57] F. He, S. Chandrasekar, N. S. V. Rao, and C. Y. T. Ma, "Effects of interdependencies on game-theoretic defense of cyber-physical infrastructures," in *International Conference on Information Fusion*, 2019.

[58] N. S. V. Rao, S. W. Poole, C. Y. T. Ma, F. He, J. Zhuang, and D. K. Y. Yau, "Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models," *Risk Analysis*, 2015.

[59] N. S. V. Rao, N. Imam, C. Y. T. Ma, K. Hausken, F. He, and J. Zhuang, "On defense strategies for system of systems using aggregated correlations," in *11th Annual IEEE International Systems Conference*, 2017.

[60] N. S. V. Rao, C. Y. T. Ma, and F. He, "Defense strategies for multi-site cloud computing server infrastructures," in *International Conference on Distributed Computing and Networking*, 2018.

[61] ——, "Defense strategies and expected capacity of high performance computing infrastructures," in *International Conference on Distributed Computing and Networking*, 2019.
[62] K. S. Trivedi and A. Bobbio, *Reliability and Availability Engineering: Modeling, Analysis, and Applications*. Cambridge University Press, Cambridge, UK, 2017.
[63] T. Bedford and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, Cambridge, UK, 2001.
[64] J. T. Blake and K. S. Trivedi, "Reliability analysis of interconnection networks using hierarchical composition," *IEEE transactions on reliability*, vol. 38, no. 1, pp. 111–120, 1989.
[65] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, July 1982. [Online]. Available: https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/
[66] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: from dependability to security," *IEEE Transactions on dependable and secure computing*, vol. 1, no. 1, pp. 48–65, 2004.
[67] B. Schneier, "Attack trees," *Dr. Dobbs journal*, vol. 24, no. 12, pp. 21–29, 1999.
[68] C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1676–1886, 2013.
[69] ——, "Scalable solutions of Markov games for smart-grid infrastructure protection," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 47–55, 2013.
[70] S. Skaperdas, "Contest success functions," *Economic Theory*, vol. 7, no. 2, pp. 283–290, 1996.
[71] B. K. Rai and R. Sarin, "Generalized contest success functions," *Economic Theory*, vol. 40, no. 1, pp. 139–149, 2009.
[72] N. S. V. Rao, C. Y. T. Ma, K. Hausken, F. He, D. K. Y. Yau, and J. Zhuang, "Defense strategies for asymmetric networked systems under composite utilities," in *IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems*, 2017.
[73] Y. Kim, J. G. Park, and J.-H. Lee, "Security threats in 5g edge computing environments," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 2020, pp. 905–907.
[74] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X16305635
[75] T. Naughton, S. Hitefield, L. Sorrillo, N. Rao, J. Kohl, W. Elwasif, J. C. Bilheux, H. Bilheux, S. Boehm, J. Kincl, S. Sen, and N. Imam, "Software framework for federated science instruments," in *Proc. of Smoky Mountains Computational Sciences and Engineering Conference*. Springer-Verlag, 2020.
[76] G. N. Sorebo and M. C. Echols, *Smart Grid Security*. CRC Press, 2012.
[77] L. Xiao, N. B. Mandayam, and H. Vincent Poor, "Prospect theoretic analysis of energy exchange among microgrids," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 63–72, 2015.
[78] F. He, C. J. Agwuegbo, N. S. V. Rao, and C. Y. T. Ma, "A sequential game of defense and attack on an interdependent system of systems," in *International Conference on Information Fusion*, 2018.
[79] F. He, J. Zhuang, and N. S. V. Rao, "Discrete game-theoretic analysis of defense in correlated cyber-physical systems," *Annals of Operations Research*, vol. 294, no. 1, pp. 741–767, 2020.
[80] T. Brown, D. Sarioz, A. Bar-Noy, T. LaPorta, D. Verma, M. Johnson, and H. Rowaihy, "Geometric considerations for distribution of sensors in ad-hoc sensor networks," City University of New York, Tech. Rep., November 2006, Computer Science Technical Reports, TR-2006014.



Nageswara S. V. Rao is a Corporate Fellow at Oak Ridge National Laboratory, where he joined in 1993. He received B. Tech from National Institute of Technology, Warangal, India, M.E. from School of Automation, Indian Institute of Science, Bangalore, India, and PhD in computer science from Louisiana State University. His research areas include high performance and quantum networking, information fusion, machine learning, and federations of science instruments. He is a Fellow of IEEE, and received 2005 IEEE Computer Society Technical Achievement Award and 2014 R&D 100 Award.

Chris Y. T. Ma is an assistant professor at The Hang Seng University of Hong Kong, where he joined in 2016. He received his BEng in Computer Engineering from The Chinese University of Hong Kong; MPhil in Computer Science and Engineering from The Chinese University of Hong Kong; and PhD in Computer Science from Purdue University, West Lafayette, IN, USA. His research interests include performance, privacy, and security study of networks and cyber-physical systems.

Fei He is an associate professor at Texas A&M University-Kingsville, where she joined in 2014. She received PhD in Industrial Engineering from the State University of New York at Buffalo. Her research areas include operations research and game theory with applications in cyber-physical systems and disaster mitigation. She is a member of INFORMS Computing Society and Decision Analysis Society.